A NOVAL SECURITY METHOD FOR IMPLANTING A PLAINTEXT ON ELLIPTIC CURVE CRYPTOGRAPHY BY USING TDMRC CODE

Ch. Bala Vijaya Durga[1], B. Prasanna Kumar[2], D. Nethaji Babu[3]

[1] Asst. Professor, Dept of CSE, PSCMR College of Engineering & Technology, Vijayawada (India)

[2] Assoc. Professor, Dept of CSE, Vikas College of Engineering & Technology, Vijayawada (India)

[3] Asst. Professor, Dept of CSE, Vikas College of Engineering & Technology, Vijayawada (India)

ABSTRACT

Now-a-days web applications are becoming very popular and there is a growth in the total amount of sensitive information which are transmitted over internet. While Encryption algorithms plays vital role in safeguarding the security of data. Elliptic Curve Cryptography (ECC) is a suitable public key encryption method which is used for key exchange, message encryption, for creating the digital signatures. This is considered as a decent alternative to RSA and other public key encryption algorithms which offers high level of security through smaller key sizes. While ECC is well-matched for applications which are run on devices with power and memory constraints like mobile (cell) phones and smartcards. Mobile SMS messages can been crypted by using ECC without corrupting the performance or presentation of mobile phones (or) devices. Elliptic curve analog of ElGamal system, the plaintext message which has been encoded into an elliptic curve earlier encryption. In this paper we discussed about different methods which has to be proposed in the literature for encrypting he characters in text message to an elliptic curve has to be examined and a new technique or process for encrypting the characters to the curve by using TDMRC code is projected. This TDMRC code is asymmetric key encryption algorithm and it is poly alphabetic. The nature of poly alphabetic has TDMRC code and it can be utilized to defeat the cryptanalysis which is based up on the letter regularities or frequencies .The projected encryption scheme will be reliable or consistent scheme and it will offer high security as the plaintext which is encrypted twice.

I. INTRODUCTION

The security in computer networks is a topic of powerful research due to the increasing use of the computers or laptops in moderntimes and their interconnection between thenetworks of all kinds and sizes, regularlyby internet. By all of these possibilities we can exchange the information and accessing the data which are stored in various databases spread around the world, organizations and home users have observed the need to define the appliances to certify that their information or data is well protected.

While a new type of computer system is thewell-knownembedded system, the courtesy of safetyexperts due to the criticality of the data or information has been exchanged by most of the devices. The usage of embedded systems has gradually increasing commonly in business, homes, and monitoring the natural phenomena. Among if there is another class of embedded systems, i.e. critical embedded systems, involves monitoring the environmental activities, agricultural systems and military organizations. These systems can require bettercarefulness in relation to the information or data collected and exchange between two devices or control bases, or the pilotage of aerial and ground vehicles which are considered as autonomous and unmanned.

However the critical embedded systems-security has becomea smooth and preferred requirement, then the exchange of data or information amongst these devices and their base of control is constant. While the security wishes to offers suitable approach each and every specific scenario and to secure the system in contradiction of malicious objects can be intentionally or easily retrieve the information or modify the operation of these devices, also considers the resource constraints.

II. RELATED WORKS

While the Maximum researches on security have been proposed an associative way, integrating the public and private key algorithms and also providing their integrity, authenticity, confidentiality and performance of their cryptographic applications. However, performance of elliptic curve algorithms has exposed to be possible for application and not only simple tasks of public key encryption, data encryption, these are frequentlyaccompanied by private key algorithms. The paper (Jena *et al.*, 2009) proposes awell-organized cryptosystem to encode long or lengthy messages. The variation is in the mathematical operations which are performed in the algorithm, but significantly reduces the difficulty of procedures, permitting its use in systems with restrictions.

Peng and Fang, 2010 compares the implementations of public key algorithms on smart cards. While the selected algorithms are RSA (Rivest, Shamir and Adleman) and ECC (Elliptic Curve Cryptography). Simply it was implemented and run on an Intel 8051. The time required for the generation of the key was around 5.2 seconds, decryption 17.1 seconds and encryption 21.3 seconds. According to the authors these values are low and reliable for the architecture addressed.

Some of the modifications have been occurred for the encrypting systems that was traditionally use public key algorithms which may provide some advantages. However in embedded systems, the boundaries of memory cache and memory storage are the factors that must be careful in the implementation of cryptographic algorithms. We can apply the ECC to scenarios of various types of limitations because, as the used key size is considerably smaller than that of RSA, the resource consumption would be correspondingly reduced. Habib *et al.*, 2009 told that the technique of replacing RSA by ECC was realisticand to reduce the resource consumptions of a particular security scheme for WiMAX and improves their performance.

Time Dependent Multiple Random Cipher Code (TDMRC Code)

Time Dependent Multiple Random Cipher Code (TDMRC)is an ASCII value based symmetric encryption method. It was designed for usage of fault tolerant hard real-time systems which prevents the attics reducing then it can be used for encrypting any text message or multimedia information or data. This Information or data is treated as a chain of ASCII characters and each of the ASCII character is replaced with TDMRC virtual or essential character. While this TDMRC character set is produced by pseudo random number generation technique. The codes will be change because of the random speed.

This code is Time Dependent and Poly Alphabetic. While the Master key is derived fromrealtime clock with accuracy to centisecond to form8digit number. The Poly Alphabetic Coefficient(P)chooses or picks the number of codes which are used correspondingthe each plain textcharacter.

Algorithm for generating the TDMRC code for encrypting messages

Step 1: Choose poly alphabetic coefficient P(usually single digitnumber)

Step2: Choose P number of subkeys, eachof4digits.

Step 3: Derives Master key by reading the system time with accuracy to centi second to form 8digitnumber.

Step 4: Each subkey is multiplied by master key, and 8 digits from the extreme right is taken from the product to form P random seeds.

Step 5: Generates P number of random series by using the P number of random seeds which is derived in the above step. The random series have 256 unique valuesinthe range0-255.

Step 6: The data to be encrypted is taken in the blocks for P number of characters, the ASCII value of each plain text character is found and it is substitute by the corresponding value in the random series which are obtained to cipher text character. The first character is substituted by the element from the first seriesand the second character from second series and soon.

Algorithm for generating the Decryption Message

Step 1: Same keys are used for encryption and to regenerate P number of random series and P random seeds with 256 unique elements.

Step 2: then take cipher text in blocks of P number of characters. The ASCII value of each and every character is originate or found and substitute each character with the string character of the serial number values in random series which are obtained for plain text character. The first character is substituted by the element from first series and second character from second series and so on.

Elliptic Curve Cryptography (ECC) andDeveloped Algorithms

The accepted three encryption schemes are based upon the three mathematical problems (Jena *etal.*, 2009): Elliptic curve discrete logarithm problem (ECDLP), Integer factorization problem (IFP),discrete logarithm problem (DLP). The latter offers a higher level of security, it operates with smaller key sizes in comparison to RSA and DSA (Digital Signature Algorithm). To achieve an appropriate level of security, RSA and DSA should use 1024-bit key size based on the time which is needed to break these figures, while the ECC needs to operate with 160-bit keys.

Moreover the smaller key size, ECC algorithm has definite advantages, such as only exponential-time attacks might be applied if the curve is wiselyselected. Even if factoring and multiplicative group discrete logarithms are cracked, the ECDL still be difficult to compute (Jena *et al.*, 2009). Beginning a comparison, the security level of an application of elliptic curves with 160-bit key is equivalent to RSA 1024-bit key size (Lenstra and Verheul, 2001).

The two algorithms were developed in this work. The method chosen for the implementation of ECC is El-Gamal, which chains the properties of the El-Gamal elliptic curve encryption method of swapping the messages. Its operation is as follows: two users must share the same elliptic curve point *P*. Each one need to choose a random number that acts as its private key and multiply the known point, obtaining *aP*, becomes its public key. At the beginning of the communication, the public key is transmitted to the other user, which has *bP* as public key and thus the private key *b*. For exchange of messages, user needs to multiply his/her own private key by the public key of the other user, obtaining *b(aP)*, and then add this result to the message encoded in an *M* number. Therefore, the message will be $M + b\ (aP)$. Whenever message is delivered to the receiver, he/she will be able to decode it by multiplying his/her private key by the public key of the other user, $(a(bP))$, and subtracting the total content, $M + b\ (AP) - (bP) = M$

III PROPOSED METHOD FOR DESCRIPTION

This proposed method uses TDMRC code to encode the characters in message to an elliptic curve. The main aim of this method is to offer a further level or next level or additional level of security in elliptic curve EIGamal system by making the use of polyalphabetic nature of TDMRC code. These characters in the particular message should be first converted into TDMRC virtual characters and this virtual characters can be encoded to the curve. The same characters in the message should be converted to virtual characters and then mapped into various points on the curve. Then these pointes could be converted to the cipher points by EIGammal encryption. The frequencies of letters in the plain text are not well-preserved in cipher text and this cryptanalysis based upon the letter frequency which can be defeated. This process is suitable for encrypting the small or short messages.

PROPOSED ALGORITHM FOR ENCODING THE PLAINTEXT TO THE CURVE:

Step 1: first you choose elliptic curve Ep (a, b)

Step 2: To make a TDMRC code

Step 3: get the first character of the plain text. So its ASCII value be ‘p1’. Substitute with the equivalent value in the first random series and let the new value be ‘p2’

Step 4: multiply p2 with 2P, where P is the polyalphabetic coefficient, choose during the making or generation of TDMRC code

Step 5: now x=p2*2P and you should to try to solve for y in the equation for getting the elliptic curve.

Step 6: the solution for y cannot be found for x in the particular elliptical curve and then solve y for x=(p2*2P) +1, x=(p2*2P)+2, x=(p2*2P)+3 and so on. You can solve until you get y

Step 7: at this point (x,y) on the particular elliptical curve which corresponds to the first character in the plain text

Step 8: This procedure can be repeated in all the other characters in the plain text.

By using the ECC EIgamal encryption we can encrypt the point (x,y) for two cipher text points and it can be send to the receiver. Then the receiver will decrypt the cipher text to the point (x,y). The next step we can decode the point (x,y) to the number p2 then apply the decryption algorithm of TDMRC for getting the plain text character.

IV CONCLUSION

However, elliptical cryptography has the capability to afford suitable security with smaller key size and it can be used for encrypting the mobile text messages. This elliptical curve E1gamal system is a secure method, so it is widely used for encrypting the text messages. In this paper we proposed a novel method for encoding a plain text message to elliptic curve which can obtain an additional level or extra level of security for elliptical curve encryption. While in this method first encrypt the plain text by using a symmetric key encryption scheme before encoding the points to the elliptic curve. By using this method the advantage is that the same characters in the plain text will be plotted to different points on the curve which can encrypted to various cipher points by using elliptic curve E1gamal encryption. The usage of TDMRC code generates encryption polyalphabetic and then the frequency attack can be conquered.

REFERENCES

1. Vivek Kaiyar, Kamlesh Datta, Syona Gupta, “ A survey on Elliptic curve Cryptography for pervasive computing Environment”, International Journal of Computer Applications, vol1, no: 10, December 2010.
2. Ch. Suneetha, D Sravana Kumar, “ Encryption of data using elliptic curve over finite fields, “ International journal of distributed and parallel systems. Vol 3, no:1, January 2012
3. Komal Agarwal, anju gera, “Elliptic curve cryptography with Hill cipher generation for secure text cryptosystem, “ International journal of computer applications”, November 2014
4. S. Maria Celestin vigila, K muneeswaran, “Implementaiton of text based cryptosystem using eliptic curve cryptography”, ICAC 2009, IEEE

5. Tarun Narayan Shankar, G. Sahoo, “ Cryptography with elliptic curves” International Journal of computer science and applications, Vol 2, No.1, April / May 2009
6. M.S. Srinath, V. Chandrasekaran, “Elliptic Curve Cryptography using Mirrored Elliptic Curves over Prime Fields”. Internaional Conference on information and knowledge Engineering, IKE 2010.
7. Jayabhaskar Muthukuru, Sathyanarayan, “Fixed and Variable Size Text Based Mapping Techniques using ECC”, Global Journal of Computer Science and Technology, Vol12, Issue 3. Feb 2012
8. Victor S. Miller, “Use of elliptic curves in cryptography”, Williams Edition. Advances in cryptology, Springer vol 218 of Lecture notes in computer science.